

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : Shunpei YAMAZAKI et al.
Serial No. : Not assigned yet
Filed : May 10, 2001
Title : COMMUNICATION SYSTEM

Art Unit : Unknown
Examiner : Unknown



Commissioner for Patents
Washington, D.C. 20231

TRANSMITTAL OF PRIORITY DOCUMENT UNDER 35 USC §119

Applicant hereby confirms his claim of priority under 35 USC §119 from the following application: Japan Application No. 2000-138095 filed May 11, 2000. A certified copy of each application from which priority is claimed is submitted herewith.

Please apply any charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: May 10, 2001

William D. Hare
William D. Hare
Reg. No. 44,739

Fish & Richardson P.C.
601 Thirteenth Street, NW
Washington, DC 20005
Telephone: (202) 783-5070
Facsimile: (202) 783-2331

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

J1033 U.S. PTO
09/852266
05/10/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

2 0 0 0 年 5 月 1 1 日

出 願 番 号
Application Number:

特 願 2 0 0 0 - 1 3 8 0 9 5

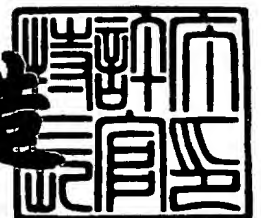
出 願 人
Applicant (s):

株式会社半導体エネルギー研究所

2 0 0 1 年 4 月 6 日

特 許 庁 長 官
Commissioner,
Patent Office

及 川 耕 造



出 証 番 号 出 証 特 2 0 0 1 - 3 0 2 6 0 5 8

【書類名】 特許願

【整理番号】 P004908

【提出日】 平成12年 5月11日

【あて先】 特許庁長官 殿

【発明者】

 【住所又は居所】 神奈川県厚木市長谷 3 9 8 番地 株式会社半導体エネルギー研究所内

 【氏名】 山崎 舜平

【発明者】

 【住所又は居所】 神奈川県厚木市長谷 3 9 8 番地 株式会社半導体エネルギー研究所内

 【氏名】 小山 潤

【特許出願人】

 【識別番号】 000153878

 【氏名又は名称】 株式会社半導体エネルギー研究所

 【代表者】 山崎 舜平

【手数料の表示】

 【予納台帳番号】 002543

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

 【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信システム

【特許請求の範囲】

【請求項 1】

使用者を識別する通信システムであって、
基準用生体情報を記憶する手段と、
前記使用者の照会用生体情報を読み取る手段と、
前記照会用生体情報を前記基準用生体情報と照合する手段と、
前記照合が合致した場合、相手先に合致したことをデータとして送る手段と、
を有することを特長とする通信システム。

【請求項 2】

使用者を識別する通信システムであって、
 n 個の基準用生体情報を記憶する手段と、
前記使用者の n 個の照会用生体情報を読み取る手段と、
前記 n 個の照会用生体情報を前記 n 個の基準用生体情報と照合する手段と、
前記照合が全て合致した場合、相手先に合致したことをデータとして送る手段
と、
を有することを特長とする通信システム。

【請求項 3】

使用者を識別する通信システムであって、
 n 個の基準用生体情報を記憶する手段と、
前記使用者の m 個の照会用生体情報を読み取る手段と、
前記 n 個の照会用生体情報を前記 m 個の基準用生体情報と照合する手段と、
前記照合において、前記 m 個の照会用生体情報の少なくとも 1 つが、前記 n 個
の照会用生体情報の少なくとも 1 つと合致している場合、相手先に合致したこと
をデータとして送る手段と、
を有することを特長とする通信システム。

【請求項 4】

使用者を識別する通信システムであって、

複数の種類の基準用生体情報を記憶する手段と、
前記使用者の複数の種類の照会用生体情報を読み取る手段と、
前記複数の照会用生体情報と前記複数の基準用生体情報とを照合する手段と、
前記照合において、前記複数の種類の照会用生体情報と、前記複数の種類の基準用生体情報と全て合致している場合、相手先に合致したことをデータとして送る手段と、
を有することを特長とする通信システム。

【請求項 5】

使用者を識別する通信システムであって、
複数の種類の基準用生体情報を n 個記憶する手段と、
前記使用者の複数の種類の照会用生体情報を m 個読み取る手段と、
前記 n 個の照会用生体情報を前記 m 個の基準用生体情報と照合する手段と、
前記照合において、前記複数の種類の照会用生体情報のうち各種類の照会用生体情報の少なくとも 1 つが、前記 m 個の基準用生体情報のうち各種類の基準用生体情報の少なくとも 1 つと合致している場合、相手先に合致したことをデータとして送る手段と、
を有することを特長とする通信システム。

【請求項 6】

使用者を識別する通信システムであって、
複数の種類の基準用生体情報を n 個記憶する手段と、
前記使用者の複数の種類の照会用生体情報を m 個読み取る手段と、
前記 n 個の照会用生体情報を前記 m 個の基準用生体情報と照合する手段と、
前記照合において、前記複数の種類の照会用生体情報の全てが、前記 m 個の基準用生体情報の全てと合致している場合、相手先に合致したことをデータとして送る手段と、
を有することを特長とする通信システム。

【請求項 7】

使用者を識別する通信システムであって、
基準用生体情報を記憶する手段と、

前記使用者の照会用生体情報を読み取る手段と、
前記照会用生体情報を前記基準用生体情報と照合する手段と、
前記照合が合致した場合、管理者に合致したことをデータとして送る手段と、
を有する通信システムであって、

前記相手先が前記照合が合致したことをデータとして受け取った後に、前記管理者を間に介して前記使用者と前記相手先との間で通信が開始されることを特長とする通信システム。

【請求項 8】

使用者を識別する通信システムであって、
基準用生体情報を記憶する手段と、
前記使用者の照会用生体情報を読み取る手段と、
前記照会用生体情報を前記基準用生体情報と照合する手段と、
前記照合が合致した場合、管理者に合致したことをデータとして送る手段と、
前記管理者は前記照合が合致したことをデータとして相手先に送る手段と、
を有する通信システムであって、

前記相手先が前記照合が合致したことをデータとして受け取った後に、前記管理者を間に介して前記使用者と前記相手先との間で通信が開始されることを特長とする通信システム。

【請求項 9】

使用者を識別する通信システムであって、
基準用生体情報を記憶する手段と、
前記使用者の照会用生体情報を読み取る手段と、
前記照会用生体情報を前記基準用生体情報と照合する手段と、
前記照合が合致した場合、管理者に合致したことをデータとして送る手段と、
前記管理者は前記照合が合致したことをデータとして相手先に送る手段と、
を有する通信システムであって、

前記相手先が前記照合が合致したことをデータとして受け取った後に、前記使用者と前記相手先との間で直接通信が開始されることを特長とする通信システム

。

【請求項 1 0】

請求項 1 乃至請求項 9 のいずれか 1 項において、前記使用者と前記相手先との間で取引が行われ、前記相手先に設定された条件を満たす場合のみ、前記使用者の識別を要求することを特長とする通信システム。

【請求項 1 1】

使用者を識別する通信システムであって、
 基準用生体情報を記憶する手段と、
 前記使用者の照会用生体情報を読み取る手段と、
 前記照会用生体情報を前記基準用生体情報と照合する手段と、
 前記照合が合致した場合、相手先に合致したことをデータとして送る手段と、
 を有する通信システムであって、

前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記基準用生体情報を書き換えられることを特長とする通信システム。

【請求項 1 2】

使用者を識別する通信システムであって、
 n 個の基準用生体情報を記憶する手段と、
 前記使用者の n 個の照会用生体情報を読み取る手段と、
 前記 n 個の照会用生体情報を前記 n 個の基準用生体情報と照合する手段と、
 前記照合が全て合致した場合、相手先に合致したことをデータとして送る手段と、
 を有する通信システムであって、

前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記 n 個の基準用生体情報を書き換えられることを特長とする通信システム。

【請求項 1 3】

使用者を識別する通信システムであって、

○

n 個の基準用生体情報を記憶する手段と、
 前記使用者の m 個の照会用生体情報を読み取る手段と、
 前記 n 個の照会用生体情報を前記 m 個の基準用生体情報と照合する手段と、
 前記照合において、前記 m 個の照会用生体情報の少なくとも 1 つが、前記 n 個の照会用生体情報の少なくとも 1 つと合致している場合、相手先に合致したことをデータとして送る手段と、
 を有する通信システムであって、

前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記 n 個の基準用生体情報を書き換えられることを特長とする通信システム。

【請求項 1 4】

使用者を識別する通信システムであって、
 複数の種類の基準用生体情報を記憶する手段と、
 前記使用者の複数の種類の照会用生体情報を読み取る手段と、
 前記複数の照会用生体情報と前記複数の基準用生体情報とを照合する手段と、
 前記照合において、前記複数の種類の照会用生体情報と、前記複数の種類の基準用生体情報と全て合致している場合、相手先に合致したことをデータとして送る手段と、
 を有する通信システムであって、

前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記複数の種類の基準用生体情報を書き換えられることを特長とする通信システム。

【請求項 1 5】

使用者を識別する通信システムであって、
 複数の種類の基準用生体情報を n 個記憶する手段と、
 前記使用者の複数の種類の照会用生体情報を m 個読み取る手段と、
 前記 n 個の照会用生体情報を前記 m 個の基準用生体情報と照合する手段と、

前記照合において、前記複数の種類の照会用生体情報のうち各種類の照会用生体情報の少なくとも1つが、前記m個の基準用生体情報のうち各種類の基準用生体情報の少なくとも1つと合致している場合、相手先に合致したことをデータとして送る手段と、

を有する通信システムであって、

前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記複数の種類の基準用生体情報を書き換えられることを特長とする通信システム。

【請求項 1 6】

使用者を識別する通信システムであって、

複数の種類の基準用生体情報をn個記憶する手段と、

前記使用者の複数の種類の照会用生体情報をm個読み取る手段と、

前記n個の照会用生体情報を前記m個の基準用生体情報と照合する手段と、

前記照合において、前記複数の種類の照会用生体情報の全てが、前記m個の基準用生体情報の全てと合致している場合、相手先に合致したことをデータとして送る手段と、

を有する通信システムであって、

前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記複数の種類の基準用生体情報を書き換えられることを特長とする通信システム。

【請求項 1 7】

使用者を識別する通信システムであって、

基準用生体情報を記憶する手段と、

前記使用者の照会用生体情報を読み取る手段と、

前記照会用生体情報を前記基準用生体情報と照合する手段と、

前記照合が合致した場合、管理者に合致したことをデータとして送る手段と、
を有する通信システムであって、



前記管理者に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記管理者に送り、前記管理者において前記パスワードが正しいと認証された場合、前記基準用生体情報を書き換えられることを特長とする通信システム。

【請求項 1 8】

請求項 1 乃至請求項 1 7 のいずれか 1 項に記載の前記基準用生体情報とは、指紋、掌紋または声紋であることを特長とする通信システム。

【請求項 1 9】

請求項 1 乃至請求項 1 8 のいずれか 1 項に記載の前記照合用生体情報とは、指紋、掌紋または声紋であることを特長とする通信システム。

【請求項 2 0】

請求項 1 8 または請求項 1 9 において、前記掌紋は手ひらの全体の掌紋、もしくは前記手のひらの一部の掌紋であることを特徴とした通信システム。

【請求項 2 1】

請求項 1 乃至請求項 2 0 のいずれか 1 項において、前記記憶する手段とは、フラッシュメモリであることを特長とする通信システム。

【請求項 2 2】

請求項 1 乃至請求項 2 1 のいずれか 1 項において、前記読み取る手段とは、フォトダイオードまたは CCD であることを特長とする通信システム。

【請求項 2 3】

請求項 1 乃至請求項 2 2 のいずれか 1 項において、
携帯情報端末を用いることを特長とする通信システム。

【請求項 2 4】

請求項 1 乃至請求項 2 2 のいずれか 1 項において、
携帯電話を用いることを特長とする通信システム。

【請求項 2 5】

請求項 1 乃至請求項 2 2 のいずれか 1 項において、
パーソナルコンピュータを用いることを特長とする通信システム。

【0 0 0 0】

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は通信システムに関する。特に、生体情報を用いて認証を行うことを特徴とした通信システムである。

【0002】

【従来の技術】

近年、携帯電話、パソコン、携帯情報端末などの認証装置を使用してインターネットに接続する通信技術が急速に発展しつつある。企業、家庭でのインターネット等への接続は、据え置き型のパソコンに電話回線を接続することで行われている。特に近年では、インターネットが簡単に出来るiモードなどの携帯電話が普及し、さまざまな情報交換が簡便に行われるようになった。

【0003】

さらに近頃では、居ながらにして取引を成立させることが可能であるという利便性の面から、インターネット等の通信網を用いた通信販売や株取引などが注目をあびている。しかし認証装置を用いて相手先と取引を行う場合、通信を行っている相手が本人であることの確認（認証作業）が難しい。そのため、本人以外の第三者が本人になりすまし、使用者として相手先と通信する可能性がある。

【0004】

上述したことに鑑み、認証作業において使用者が本人であることの確実性を高めることが求められている。

【0005】

図14に従来の認証作業のフローを示す。まず使用者は、携帯電話等の認証装置を用いてインターネットに接続し、指定された条件下で、認証のための暗証番号等のパスワードをデータとして相手先に送信する。認証のためのパスワードをデータとして受信した相手先は、自分のところにあらかじめ登録された本人のパスワードと、使用者から送られてきたパスワードとの照合を行い、合致するかどうかを確認する。ここで合致が見られれば、使用者は本人であるということが認証され、合致しない場合は認証されない。

【 0 0 0 6 】

照合が終了した後、相手先は認証の是非を情報として有する照合終了信号を、使用者にデータとして送信する。使用者が本人として認証されなかった場合は、使用者は再びパスワードをデータとして相手先に送信する。また認証された場合は、照合終了信号を受信した時点で認証作業が終了し、次に通信が開始される。

【 0 0 0 7 】

なお本明細書において通信とは、認証作業が終了した後に行われる、目的とする情報の送受信を意味する。

【 0 0 0 8 】

このように従来の認証作業では、本人以外の第三者が本人になりすまし、使用者として相手先と通信することを防止するために、使用者が相手先に送信した番号と、あらかじめ相手先に登録されている本人のパスワードとを照合することで、使用者が本人であることの確認が行われていた。

【 0 0 0 9 】

【発明が解決しようとする課題】

上述したような従来の認証装置を用いた通信システムでは以下の問題があった。

【 0 0 1 0 】

まず、パスワードが第三者に漏洩する可能性のあることは否めない。第三者にパスワードが漏洩した場合、従来の認証作業では使用者が本人であるという確認をすることが不可能になる。

【 0 0 1 1 】

またパスワードは本人が忘れてしまう可能性がある。その場合、本人が相手先にパスワードを問い合わせたり、パスワードを頻繁に書き換えたりする必要が生じ、非常に煩わしい。

【 0 0 1 2 】

また、従来の認証作業では、使用者は、パスワードをデータとして相手先へ送り、照合終了信号を相手先から受信する必要がある。そして、使用者が間違ったパスワードを相手先に送った場合、正しいパスワードを再び相手先に送る必要が

ある。このため、相手先と使用者との間で少なくとも2回はデータの送受信を行うことになる。

【0013】

使用者と相手先との間でデータを送受信する回数が多いと、認証作業に必要なコストが上昇する。またデータを送受信する回数が多いと、何らかのエラーによりデータの送受信中に使用者と相手先の間の回線が途切れる可能性が高くなる。データの送受信中に回線が途切れると、認証作業を最初から再び行う必要が生じ、作業が繁雑である。

【0014】

本発明は、上記問題を解決することを課題とする。

【0015】

【課題を解決するための手段】

本発明では認証作業を使用者の側のみにいて行い、相手先には認証が終了したことをデータとして送信する。そして本人かどうかの確認（識別）は、使用者の生体情報（照合用生体情報）と本人の生体情報（基準用生体情報）とを照合することで行う。

【0016】

本明細書において生体情報とは、人間が生まれつき持っている身体的な特徴で、なおかつ人間の個体識別が可能な情報を意味する。代表的な生体情報としては、指紋、掌紋、声紋等が挙げられる。なお本発明で用いられる生体情報は指紋、掌紋、声紋に限定されない。人間が生まれつき持っている身体的な特徴で、なおかつ人間の個体識別が可能な情報であれば、生体情報として本発明の認証作業に用いることが可能である。

【0017】

照合の結果、使用者と本人の生体情報が合致しない場合、使用者は再び使用者と本人の生体情報の照合を行う。使用者と本人の生体情報が合致した場合、認証が終了したことを相手先にデータとして送信し、認証作業が完了する。

【0018】

認証作業が終了し、使用者が本人であることを相手先が確認したら、相手先と

の目的とする通信が開始される。

【 0 0 1 9 】

上述した認証作業において、使用者の生体情報が本人の生体情報と合致しない場合、再び使用者の生体情報と本人の生体情報とを照合することができる。そして繰り返し照合を行おうとしたとき、連続して n 回以上（ n は自然数）合致しない場合は相手先に自動的に n 回以上合致しなかったことを通知するようにしても良い。

【 0 0 2 0 】

また、本人の生体情報（基準用生体情報）は複数あっても良く、例えば、指紋と声紋の両方を用いて認証作業を行う構成にしても良い。または、複数の指紋を本人の生体情報（基準用生体情報）として用いることも可能である。

【 0 0 2 1 】

そして使用者の生体情報（照合用生体情報）も複数用いることが可能であり、同じ種類の複数の生体情報を用いたり、種類の異なる複数の生体情報を用いたりすることが可能である。

【 0 0 2 2 】

そして基準用生体情報を書き換える場合、本人であることを確認できるものを相手先に提示することが必要である。または、一度認証作業を行った後、相手先に生体情報を書き換える際に必要なパスワードをデータとして送り、相手先においてパスワードが合致したら、基準用生体情報を書き換えることができるようにしても良い。

【 0 0 2 3 】

なお上述した認証作業は、使用者と相手先との二者間で行われる場合に限られない。例えば使用者と相手先との間の通信を管理する管理者が存在する場合、使用者が本人であるという認証が終了したことを管理者に通知することで、使用者と相手先との間の通信が開始されるようにしても良い。

【 0 0 2 4 】

この場合、使用者の生体情報と本人の生体情報の照合が連続して n 回以上（ n は自然数）合致しないと、管理者に n 回以上合致しなかったことを自動的に通知

するようにしても良い。

【 0 0 2 5 】

またこの場合、基準用生体情報を書き換える時、本人であることを確認できるものを管理者に提示することが必要である。または、一度認証作業を行った後、管理者に生体情報を書き換える際に必要なパスワードをデータとして送り、管理者側においてパスワードが合致したら、基準用生体情報を書き換えることができるようにしても良い。

【 0 0 2 6 】

上述したように、本発明は生体情報を用いて認証作業を行うため、パスワードが本人以外の第三者に漏洩して、本人であることの確認が行われなくなる可能性がなくなる。よって、認証作業によって使用者が本人であることの確実性を高くすることができる。

【 0 0 2 7 】

そして、認証作業の際に、使用者と相手先（または管理者）との間においてデータをやりとりする回数が抑えられるため、データの送受信に必要なコストを抑えることができ、何らかのエラーにより通信が途絶えて認証作業を再び最初から行うという繁雑さを回避することができる。

【 0 0 2 8 】

さらに、使用者の生体情報を用いて認証作業を行うため、使用者がパスワードを忘れて相手先に問い合わせたり、パスワードを頻繁に書き換えたりする必要がなくなる。

【 0 0 2 9 】

また一般的に生体情報は、パスワードに比べて情報量が大きい。しかし本発明では、本人または使用者の生体情報を、データとして相手先（または管理者）に直接送信する必要がないので、相手先（または管理者）とのデータの送受信に必要な時間の長さを抑えることができ、コストも抑えることができる。

【 0 0 3 0 】

また本発明では、認証作業を行う全ての人の基準用生体情報を、相手先（または管理者）が保存しておく必要がないので、生体情報の情報量がパスワードに比

べて大きくても、相手先（または管理者）の負担が重くなることがない。そして、個人で基準用生体情報を保存しているので、セキュリティが破られたときに漏洩する基準用生体情報の数（この場合、同一の人が有する全ての生体情報を一と数える）を、認証作業を行う全ての人の基準用生体情報を相手先（または管理者）に保存しておく場合に比べて、抑えることが可能である。

【 0 0 3 1 】

以下に本発明の構成を示す。

【 0 0 3 2 】

本発明は使用者を識別する通信システムであって、
基準用生体情報を記憶する手段と、
前記使用者の照会用生体情報を読み取る手段と、
前記照会用生体情報を前記基準用生体情報と照合する手段と、
前記照合が合致した場合、相手先に合致したことをデータとして送る手段と、
を有することを特長とする。

【 0 0 3 3 】

本発明は使用者を識別する通信システムであって、
 n 個の基準用生体情報を記憶する手段と、
前記使用者の n 個の照会用生体情報を読み取る手段と、
前記 n 個の照会用生体情報を前記 n 個の基準用生体情報と照合する手段と、
前記照合が全て合致した場合、相手先に合致したことをデータとして送る手段と、
を有することを特長とする。

【 0 0 3 4 】

本発明は使用者を識別する通信システムであって、
 n 個の基準用生体情報を記憶する手段と、
前記使用者の m 個の照会用生体情報を読み取る手段と、
前記 n 個の照会用生体情報を前記 m 個の基準用生体情報と照合する手段と、
前記照合において、前記 m 個の照会用生体情報の少なくとも 1 つが、前記 n 個の照会用生体情報の少なくとも 1 つと合致している場合、相手先に合致したこと

をデータとして送る手段と、
を有することを特長とする。

【 0 0 3 5 】

本発明は使用者を識別する通信システムであって、
複数の種類の基準用生体情報を記憶する手段と、
前記使用者の複数の種類の照会用生体情報を読み取る手段と、
前記複数の照会用生体情報と前記複数の基準用生体情報とを照合する手段と、
前記照合において、前記複数の種類の照会用生体情報と、前記複数の種類の基準用生体情報と全て合致している場合、相手先に合致したことをデータとして送る手段と、
を有することを特長とする。

【 0 0 3 6 】

本発明は使用者を識別する通信システムであって、
複数の種類の基準用生体情報を n 個記憶する手段と、
前記使用者の複数の種類の照会用生体情報を m 個読み取る手段と、
前記 n 個の照会用生体情報を前記 m 個の基準用生体情報と照合する手段と、
前記照合において、前記複数の種類の照会用生体情報のうち各種類の照会用生体情報の少なくとも 1 つが、前記 m 個の基準用生体情報のうち各種類の基準用生体情報の少なくとも 1 つと合致している場合、相手先に合致したことをデータとして送る手段と、
を有することを特長とする。

【 0 0 3 7 】

本発明は使用者を識別する通信システムであって、
複数の種類の基準用生体情報を n 個記憶する手段と、
前記使用者の複数の種類の照会用生体情報を m 個読み取る手段と、
前記 n 個の照会用生体情報を前記 m 個の基準用生体情報と照合する手段と、
前記照合において、前記複数の種類の照会用生体情報の全てが、前記 m 個の基準用生体情報の全てと合致している場合、相手先に合致したことをデータとして送る手段と、

を有することを特長とする。

【 0 0 3 8 】

本発明は使用者を識別する通信システムであって、
 基準用生体情報を記憶する手段と、
 前記使用者の照会用生体情報を読み取る手段と、
 前記照会用生体情報を前記基準用生体情報と照合する手段と、
 前記照合が合致した場合、管理者に合致したことをデータとして送る手段と、
 を有する通信システムであって、
 前記相手先が前記照合が合致したことをデータとして受け取った後に、前記管理者を間に介して前記使用者と前記相手先との間で通信が開始されることを特長とする。

【 0 0 3 9 】

本発明は使用者を識別する通信システムであって、
 基準用生体情報を記憶する手段と、
 前記使用者の照会用生体情報を読み取る手段と、
 前記照会用生体情報を前記基準用生体情報と照合する手段と、
 前記照合が合致した場合、管理者に合致したことをデータとして送る手段と、
 前記管理者は前記照合が合致したことをデータとして相手先に送る手段と、
 を有する通信システムであって、
 前記相手先が前記照合が合致したことをデータとして受け取った後に、前記管理者を間に介して前記使用者と前記相手先との間で通信が開始されることを特長とする。

【 0 0 4 0 】

本発明は使用者を識別する通信システムであって、
 基準用生体情報を記憶する手段と、
 前記使用者の照会用生体情報を読み取る手段と、
 前記照会用生体情報を前記基準用生体情報と照合する手段と、
 前記照合が合致した場合、管理者に合致したことをデータとして送る手段と、
 前記管理者は前記照合が合致したことをデータとして相手先に送る手段と、

を有する通信システムであって、

前記相手先が前記照合が合致したことをデータとして受け取った後に、前記使用者と前記相手先との間で直接通信が開始されることを特長とする。

【 0 0 4 1 】

前記使用者と前記相手先との間で取引が行われ、前記相手先に設定された条件を満たす場合のみ、前記使用者の識別を要求することを特長としても良い。

【 0 0 4 2 】

本発明は使用者を識別する通信システムであって、

基準用生体情報を記憶する手段と、

前記使用者の照会用生体情報を読み取る手段と、

前記照会用生体情報を前記基準用生体情報と照合する手段と、

前記照合が合致した場合、相手先に合致したことをデータとして送る手段と、
を有する通信システムであって、

前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記基準用生体情報を書き換えられることを特長とする。

【 0 0 4 3 】

本発明は使用者を識別する通信システムであって、

n 個の基準用生体情報を記憶する手段と、

前記使用者の n 個の照会用生体情報を読み取る手段と、

前記 n 個の照会用生体情報を前記 n 個の基準用生体情報と照合する手段と、

前記照合が全て合致した場合、相手先に合致したことをデータとして送る手段と、

を有する通信システムであって、

前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記 n 個の基準用生体情報を書き換えられることを特長とする。

【 0 0 4 4 】

本発明は使用者を識別する通信システムであって、
n 個の基準用生体情報を記憶する手段と、
前記使用者の m 個の照会用生体情報を読み取る手段と、
前記 n 個の照会用生体情報を前記 m 個の基準用生体情報と照合する手段と、
前記照合において、前記 m 個の照会用生体情報の少なくとも 1 つが、前記 n 個の照会用生体情報の少なくとも 1 つと合致している場合、相手先に合致したことをデータとして送る手段と、
を有する通信システムであって、
前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記 n 個の基準用生体情報を書き換えられることを特長とする。

【 0 0 4 5 】

本発明は使用者を識別する通信システムであって、
複数の種類の基準用生体情報を記憶する手段と、
前記使用者の複数の種類の照会用生体情報を読み取る手段と、
前記複数の照会用生体情報と前記複数の基準用生体情報とを照合する手段と、
前記照合において、前記複数の種類の照会用生体情報と、前記複数の種類の基準用生体情報と全て合致している場合、相手先に合致したことをデータとして送る手段と、
を有する通信システムであって、
前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記複数の種類の基準用生体情報を書き換えられることを特長とする。

【 0 0 4 6 】

本発明は使用者を識別する通信システムであって、
複数の種類の基準用生体情報を n 個記憶する手段と、
前記使用者の複数の種類の照会用生体情報を m 個読み取る手段と、

前記 n 個の照会用生体情報を前記 m 個の基準用生体情報と照合する手段と、

前記照合において、前記複数の種類の照会用生体情報のうち各種類の照会用生体情報の少なくとも 1 つが、前記 m 個の基準用生体情報のうち各種類の基準用生体情報の少なくとも 1 つと合致している場合、相手先に合致したことをデータとして送る手段と、

を有する通信システムであって、

前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記複数の種類の基準用生体情報を書き換えられることを特長とする。

【 0 0 4 7 】

本発明は使用者を識別する通信システムであって、

複数の種類の基準用生体情報を n 個記憶する手段と、

前記使用者の複数の種類の照会用生体情報を m 個読み取る手段と、

前記 n 個の照会用生体情報を前記 m 個の基準用生体情報と照合する手段と、

前記照合において、前記複数の種類の照会用生体情報の全てが、前記 m 個の基準用生体情報の全てと合致している場合、相手先に合致したことをデータとして送る手段と、

を有する通信システムであって、

前記相手先に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記相手先に送り、前記相手先において前記パスワードが正しいと認証された場合、前記複数の種類の基準用生体情報を書き換えられることを特長とする。

【 0 0 4 8 】

本発明は使用者を識別する通信システムであって、

基準用生体情報を記憶する手段と、

前記使用者の照会用生体情報を読み取る手段と、

前記照会用生体情報を前記基準用生体情報と照合する手段と、

前記照合が合致した場合、管理者に合致したことをデータとして送る手段と、

を有する通信システムであって、

前記管理者に前記照合が合致したことをデータとして送った後に、パスワードをデータとして前記管理者に送り、前記管理者において前記パスワードが正しいと認証された場合、前記基準用生体情報を書き換えられることを特長とする通信システム。

【0049】

前記基準用生体情報が、指紋、掌紋または声紋であることを特長としていても良い。

【0050】

前記照合用生体情報が、指紋、掌紋または声紋であることを特長としていても良い。

【0051】

前記掌紋は手ひらの全体の掌紋、もしくは前記手のひらの一部の掌紋であることを特徴としていても良い。

【0052】

前記記憶する手段が、フラッシュメモリであることを特長としていても良い。

【0053】

前記読み取る手段が、フォトダイオードまたはCCDであることを特長としていても良い。

【0054】

本発明は、携帯情報端末、携帯電話またはパーソナルコンピュータを用いることを特長としていても良い。

【0055】

【発明の実施の形態】

図1に本発明の通信システムのフローを示す。認証作業が開始されると、認証作業を行う装置（認証装置）によって使用者の生体情報が採取される。生体情報の採取は、使用者が認証装置を制御することで開始される。あらかじめプログラムされていれば、1つの操作用のキー（操作キー）を押すことによって生体情報の採取が開始されるようにすることも可能である。また、認証装置の電源投入時

に自動的に生体情報の採取がはじめられるようにすることも可能である。

【 0 0 5 6 】

生体情報の採取は、例えば、CCDやフォトダイオードを用いたラインセンサーやエリアセンサー、マイク等によって行われる。

【 0 0 5 7 】

認証装置には、あらかじめ本人の生体情報（基準用生体情報）が記憶されている。基準用生体情報は、例えば認証装置が有する、不揮発性メモリなどで形成されている内蔵メモリに蓄えられている。

【 0 0 5 8 】

採取された使用者の生体情報（照合用生体情報）は、あらかじめ認証装置に記憶されている本人の生体情報（基準用生体情報）と照合される。ここで、照合用生体情報と基準用生体情報の2つの生体情報が合致すると判断されれば、使用者は目的とする通信を行う本人であることが認証される。

【 0 0 5 9 】

ここで照合が合致しないと判断された場合、認証装置によって再び使用者の生体情報を採取し、採取した照合用生体情報と基準用生体情報を再度照合することが可能である。

【 0 0 6 0 】

なお使用者が生体情報の照合をやり直す回数は、実施者が任意に設定することができる。例えば一度の認証作業中にn回（nは任意の自然数）より多く繰り返して照合を行うことができないようにしても良い。また、n回連続して照合が合致しなかった場合、認証装置がアラームを発するようにしても良い。また、n回連続して照合が合致しなかったことを、使用者以外の人間または該認証装置以外の装置に、自動的に通知する様にしても良い。

【 0 0 6 1 】

認証完了後、認証が完了したという情報を有する信号（認証完了信号）を、目的とする通信を行う相手先に送信する。このとき、認証はすでに完了しているので、新たに相手先との間で生体情報のやりとりを行う必要がなく、相手先は認証装置から認証完了信号を受信するだけでよい。

【 0 0 6 2 】

相手先が認証完了信号を受信した時点で、認証作業が終了する。認証作業が終了した後、使用者と相手先との間で、目的とする通信が行われる。なお目的とする通信は、取引等の営利のためになす経済行為に用いられることに限定されない。使用者と相手先との間で行われる通信は、あらゆる意志や情報の伝達が可能である。

【 0 0 6 3 】

なお、本発明において認証装置は、使用者の生体情報の採取と、生体情報の照合と、認証完了信号の送信といった、3つの機能を有していることが必要である。1つの認証装置が上記3つの機能を併せ持っていても良い。また複数の装置を用いて上記3つの機能を果たすようにしても良い。この場合、複数の装置を全て合わせて認証装置と呼ぶ。

【 0 0 6 4 】

次に、本発明の通信システムに用いられる生体情報のうち、指紋及び掌紋について説明する。

【 0 0 6 5 】

図2に人間の右手の図を示す。生体情報として認証装置に読み取られるのは、手のひらの一部である掌紋1、手のひら全体である掌紋2、親指の指紋、人差し指の指紋、中指の指紋、薬指の指紋または小指の指紋である。また右手ではなく左手の掌紋を用いても良く、右手と左手を両方用いても良い。

【 0 0 6 6 】

手のひらの一部である掌紋1、手のひら全体である掌紋2、親指の指紋、人差し指の指紋、中指の指紋、薬指の指紋及び小指の指紋は、個々の人間に特有のものであるため、第3者による認証装置の悪用を防ぐことができる。

【 0 0 6 7 】

なお生体情報のうち、1種類だけ本発明の通信システムに用いても良いし、複数種類用いても良い。また、同じ種類の生体情報を単数または複数用いることもできる。例えば同じ親指の指紋を複数生体情報として用いることが可能である。また、異なる種類の生体情報を複数用いることができる。例えば同じ小指の指紋

を複数と、声紋とを共に生体情報として用いることが可能である。

【 0 0 6 8 】

以下に、同じ種類の複数の生体情報を用いて照合を行う場合について、具体的に説明する。

【 0 0 6 9 】

図 3 に複数の基準用生体情報を用いた場合の照合の関係図を示す。図 3 (A) では、4 つの基準用生体情報 (A 1、A 2、A 3、A 4) と、同じく 4 つの照合用生体情報 (A 1'、A 2'、A 3'、A 4') とが全て合致した場合に認証される例を示す。

【 0 0 7 0 】

図 3 (A) に示すように、A 1 と A 1'、A 2 と A 2'、A 3 と A 3'、A 4 と A 4' がそれぞれ合致している。このように、複数の基準用生体情報と複数の照合用生体情報とが全て合致してはじめて認証されるようにすることで、使用者が本人であることの確実性を高めることができる。

【 0 0 7 1 】

なお基準用生体情報と照合用生体情報の数は 4 つに限定されず、生体情報の数は任意である。

【 0 0 7 2 】

図 3 (B) では、4 つの基準用生体情報 (A 1、A 2、A 3、A 4) のいずれか 1 つと、照合用生体情報 (A 5'、A 6'、A 7'、A 2') のいずれか 1 つとが合致した場合に認証される例を示す。

【 0 0 7 3 】

図 3 (B) に示すように、A 2 と A 2' が合致しているが、A 1、A 3、A 4 と、A 5'、A 6'、A 7' とは合致していない。このように、複数の基準用生体情報のいずれか 1 つと、複数の照合用生体情報のいずれか 1 つとが合致してはじめて認証されるようにすることで、照合用生体情報を採取する回数を抑えることができ、認証作業が容易になる。

【 0 0 7 4 】

なお基準用生体情報と照合用生体情報の数は 4 つに限定されず、生体情報の数

は任意である。また図 3 (B) では、複数の基準用生体情報のいずれか 1 つと、複数の照合用生体情報のいずれか 1 つとが合致してはじめて認証される様になっているが、合致する数は 1 つに限定されない。合致するべき数は実施者が任意に設定することが可能である。

【 0 0 7 5 】

図 4 に複数種類の基準用生体情報を用いた場合の照合の関係図を示す。図 4 (A) では、2 種類の基準用生体情報 (A 1、A 2、A 3、B 1、B 2) と、同じく 2 種類の照合用生体情報 (A 1'、A 2'、A 3'、B 1'、B 2') とが全て合致した場合に認証される例を示す。

【 0 0 7 6 】

図 4 (A) に示すように、A 1 と A 1'、A 2 と A 2'、A 3 と A 3'、B 1 と B 1'、B 2 と B 2' がそれぞれ合致している。このように、複数種類の基準用生体情報と複数種類の照合用生体情報とが全て合致して、はじめて認証されるようにすることで、使用者が本人であることの確実性を高めることができる。

【 0 0 7 7 】

なお基準用生体情報と照合用生体情報の種類は 2 つに限定されず、生体情報の種類の数は任意である。また基準用生体情報と照合用生体情報の各種類の数も任意である。

【 0 0 7 8 】

図 4 (B) では、3 つの基準用生体情報 (A 1、A 2、A 3) のいずれか 1 つと、照合用生体情報 (A 4'、A 5'、A 2') のいずれか 1 つとが合致し、2 つの基準用生体情報 (B 1、B 2) のどちらか 1 つと、照合用生体情報 (B 3'、B 1') のどちらか 1 つとが合致した場合に認証される例を示す。

【 0 0 7 9 】

図 4 (B) に示すように、A 2 と A 2'、B 1 と B 1' が合致しているが、A 1、A 3、B 2 と、A 4'、A 5'、B 3' は合致していない。このように複数種の基準用生体情報を用い、各種類ごとに、基準用生体情報のいずれか 1 つと、照合用生体情報のいずれか 1 つとが合致して、はじめて認証されるようにすることで、使用者が本人であることの確実性を高めることができる。

【 0 0 8 0 】

なお基準用生体情報と照合用生体情報の種類は2つに限定されず、生体情報の種類の数は任意である。また基準用生体情報と照合用生体情報の各種類の数も任意である。また図4（B）では、各種類ごとに基準用生体情報のいずれか1つと、複数の照合用生体情報のいずれか1つとが合致してはじめて認証される様になっているが、合致する数は1つに限定されない。生体情報の各種類毎に合致するべき数は実施者が任意に設定することが可能である。

【 0 0 8 1 】

次に、上述した認証作業において、認証が完了した後のフローについて、図5を用いて詳しく説明する。

【 0 0 8 2 】

図5（A）は、認証作業と通信とが、使用者と相手先との二者間でのみ行われる場合の関係図である。認証が完了した後、使用者側（具体的には使用者が用いる認証装置）から相手先に、認証終了信号が送信される。そして使用者と、相手先との間で目的とする通信が開始される。

【 0 0 8 3 】

図5（B）は、認証作業と通信が、使用者と相手先との二者間でのみ行われるのではなく、使用者と、相手先と、管理者との三者間で行われる場合の関係図である。管理者は、使用者と相手先との間の通信を管理する役目を担っている。

【 0 0 8 4 】

認証が完了するまでのフローは、使用者と相手先との二者間で行われる場合と同じなので省略する。使用者が本人であるという認証が完了したら、使用者側（具体的には使用者が用いる認証装置）から管理者に、認証終了信号が送信される。そして管理者を介して、使用者と相手先との間で目的とする通信が開始される。

【 0 0 8 5 】

図5（C）は、図5（B）と同じく認証作業と通信が使用者と、相手先と、管理者との三者間で行われる場合の関係図である。

【 0 0 8 6 】

認証が完了するまでのフローは、使用者と相手先との二者間で行われる場合と同じなので省略する。使用者が本人であるという認証が完了したら、使用者側（具体的には使用者が用いる認証装置）から管理者に認証終了信号が送信される。管理者は、使用者側からの認証終了信号を受信したら、相手先にも認証終了信号を送信する。そして管理者を介して、使用者と相手先との間で目的とする通信が開始される。

【0087】

図5（D）は、図5（B）、図5（C）と同じく、認証作業と通信が使用者と、相手先と、管理者との三者間で行われる場合の関係図である。

【0088】

認証が完了するまでのフローは、使用者と相手先との二者間で行われる場合と同じなので省略する。使用者が本人であるという認証が完了したら、使用者側（具体的には使用者が用いる認証装置）から管理者に認証終了信号が送信される。管理者は、使用者側からの認証終了信号を受信したら、相手先にも認証終了信号を送信する。そして使用者と相手先との間で、管理者を介さずに直接、目的とする通信が開始される。

【0089】

なお本発明の通信システムにおいて、使用者と相手先以外にも認証作業と通信に関与しているもの（例えば管理者）が存在する場合、認証が完了したあとのフローは、さまざまな組み合わせが考えられる。本発明は図5に示した関係図に限定されない。使用者が認証完了信号を他者に送信することで、使用者と相手先との通信を開始することが可能であるならば、どのような組み合わせでも良い。

【0090】

また本発明の通信システムにおいて、相手先と管理者の数は1つに限定されない、相手先が複数存在していても良いし、管理者が複数存在していても良い。

【0091】

上述したように、本発明は生体情報を用いて認証作業を行うため、パスワードが本人以外の第三者に漏洩して、本人であることの確認が行われなくなる可能性がなくなる。よって、認証作業によって使用者が本人であることの確実性を高く

○
することができる。

【0092】

そして、認証作業の際に、使用者と相手先（または管理者）との間においてデータをやりとりする回数が抑えられるため、データの送受信に必要なコストを抑えることができ、何らかのエラーにより通信が途絶えて認証作業を再び最初から行うという繁雑さを回避することができる。

【0093】

さらに、使用者の生体情報を用いて認証作業を行うため、使用者がパスワードを忘れて相手先に問い合わせたり、パスワードを頻繁に書き換えたりする必要がなくなる。

【0094】

また一般的に生体情報は、パスワードに比べて情報量が大きい。しかし本発明では、本人または使用者の生体情報を、データとして相手先（または管理者）に直接送信する必要がないので、相手先（または管理者）とのデータの送受信に必要な時間の長さを抑えることができ、コストも抑えることができる。

【0095】

また本発明では、認証作業を行う全ての人の基準用生体情報を、相手先（または管理者）が保存しておく必要がないので、生体情報の情報量がパスワードに比べて大きくても、相手先（または管理者）の負担が重くなることがない。そして、個人で基準用生体情報を保存しているので、セキュリティが破られたときに漏洩する基準用生体情報の数（この場合、同一の人が有する全ての生体情報を一と数える）を、認証作業を行う全ての人の基準用生体情報を相手先（または管理者）に保存しておく場合に比べて、抑えることが可能である。

【0096】

【実施例】

以下に、本発明の実施例について説明する。

【0097】

（実施例1）

本実施例では、認証装置に記憶されている基準用生体情報を、認証装置を用い

て書き換える場合について詳しく説明する。

【0098】

図6に本実施例の、基準用生体情報の書き換えのフローを示す。まず、認証作業を行い、使用者が本人であることを認証する。なお認証作業の詳しい説明については実施の形態において既に示したので、ここでは説明を省略する。

【0099】

認証作業が終了し使用者と相手先（または管理者）との通信が開始されたら、書き換え作業が開始され、生体情報を書き換える際に必要なパスワードを、使用者が相手先にデータとして送信する。

【0100】

このパスワードの照合において合致しない場合は、基準用生体情報の書き換えができない。この場合、相手先（管理者）から使用者に、パスワードが合致しなかったことが通知される。そして使用者は再びパスワードをデータとして送信し直すことが可能である。

【0101】

なおこの場合も認証作業の照合の場合と同じく、パスワードを送信し直す回数は、実施者が任意に設定することができる。例えば一度の書き換え作業中にn回（nは任意の自然数）より多く繰り返して照合を行うことができないようにしても良い。また、n回連続して照合が合致しなかった場合、認証装置がアラームを発するようにしても良い。また、n回連続して照合が合致しなかったことを、使用者以外の人間または該認証装置以外の装置に、自動的に通知する様にしても良い。

【0102】

相手先においてパスワードを照合して合致したら、基準用生体情報の書き換えが承諾される。相手先（管理者）から基準用生体情報の書き換えが承諾されたことを情報として有する、書き換え承諾信号が使用者に送信される。

【0103】

使用者は、書き換え承諾信号を受信したら、認証装置に新たに生体情報を読み込む。そして新しい基準用生体情報が認証装置に記憶され、基準用生体情報の書

き換え作業が完了する。

【0104】

上述したフローに従って基準用生体情報を書き換えることで、本人以外の第三者に基準用生体情報を勝手に書き換えられてしまう可能性を低くすることができる。

【0105】

また書き換え作業の全てを、認証装置を用いて行うことができるので、基準用生体情報の書き換えの煩雑さを抑えることができる。

【0106】

(実施例2)

以下に本発明において用いられる認証装置の構成と、その動作について説明する。

【0107】

図7は本実施例の認証装置のブロック図である。本実施例の認証装置はアンテナ601、送信受信回路602、信号を圧縮伸張化、符号化する信号処理回路603、制御用マイコン604、フラッシュメモリ605、操作キー606などを有している。そしてさらに、センサー611、照合回路部612などを有している。

【0108】

操作キー606を操作することによって、制御用マイコン604がセンサー611を制御し、使用者の生体情報を読み取らせる。なお本実施例では、生体情報として掌紋または指紋を用いる例について説明する。センサー611で読み取った使用者の生体情報は、照合回路部612に入力される。

【0109】

照合回路部612に入力された使用者の生体情報（照合用生体情報）は、A/Dコンバータ613においてデジタル信号に変換される。デジタル信号に変換された使用者の生体情報は、DSP（デジタルシグナルプロセッサ）614に入力され、信号処理される。信号処理とは具体的には、生体情報をより判別しやすくするため、微分フィルタなどを用い映像の濃淡が変わるところを際立たせること

である。得られた照合用生体情報は DSP 6 1 4 内部で数値化され、比較回路 6 1 5 に入力される。

【0 1 1 0】

比較回路 6 1 5 はフラッシュメモリ 6 0 5 に記憶されている基準用生体情報と、DSP 6 1 4 内部で数値化され比較回路 6 1 5 に入力された照合用生体情報とを比較し照合する。

【0 1 1 1】

生体情報を照合する方法としては、基準用生体情報と照合用生体情報のそれぞれの特徴を比較して照合する特徴照合方式と、該二つの生体情報を直接比較する画像マッチング方式があるが、どちらの方式を用いても良い。また基準用生体情報は 1 つだけではなく、手の向きを多少変えるなどして、複数備えたほうがより確実な認証が可能となる。

【0 1 1 2】

ここで合致が見られれば、制御用マイコン 6 0 4 は認証完了信号を出力し、該認証完了信号は、信号処理回路 6 0 3、送受信回路 6 0 2、アンテナ 6 0 1 を介して認証装置から出力される。認証装置から出力された認証完了信号は、インターネットなどを通じて相手先（または管理者）に送信される。なお、認証装置から出力された認証完了信号を、インターネットを介さず直接相手先（または管理者）に送信に送信しても良い。

【0 1 1 3】

（実施例 3）

以下に本発明において用いられる認証装置の構成と、その動作の、実施例 1 とは異なる例について説明する。

【0 1 1 4】

図 8 は本実施例の認証装置のブロック図である。この認証装置はアンテナ 5 0 1、送信受信回路 5 0 2、信号を圧縮伸張化、符号化する信号処理回路 5 0 3、制御用マイコン 5 0 4、フラッシュメモリ 5 0 5、操作キー 5 0 6 などを有している。そしてさらに、マイク 5 1 1、アンプ 5 1 6、照合回路部 5 1 2 などを有している。

【 0 1 1 5 】

操作キー 5 0 6 を操作することによって、制御用マイコン 5 0 4 がマイク 5 1 1 を制御し、使用者の生体情報を読み取らせる。なお本実施例では、生体情報として、声紋を用いる例について説明する。マイク 5 1 1 で読み取った使用者の生体情報は、アンプ 5 1 6 によって増幅され、照合回路部 5 1 2 に入力される。

【 0 1 1 6 】

照合回路部 5 1 2 に入力された使用者の生体情報（照合用生体情報）は、A / D コンバータ 5 1 3 においてデジタル信号に変換される。デジタル信号に変換された照合用生体情報は、DSP（デジタルシグナルプロセッサ）5 1 4 に入力され、信号処理される。信号処理とは、具体的には、生体情報をより判別しやすくするため、帯域フィルタなどを用い、周波数ごとの音の強さを数値化することである。DSP 5 1 4 により数値化された基準用生体情報は比較回路 5 1 5 に入力される。

【 0 1 1 7 】

比較回路 5 1 5 はフラッシュメモリ 5 0 5 に記憶されている基準用生体情報と、DSP 5 1 4 内部で数値化され比較回路 5 1 5 に入力された照合用生体情報とを比較し照合する。

【 0 1 1 8 】

生体情報を照合する方法としては、基準用生体情報と照合用生体情報のそれぞれの特徴を比較して照合する特徴照合方式と、該二つの生体情報が有するスペクトルを直接比較する画像マッチング方式があるが、どちらの方式を用いても良い。また基準用生体情報は 1 つだけではなく、発音を多少変えるなどして、複数備えたほうがより確実な認証が可能となる。

【 0 1 1 9 】

ここで合致が見られれば、制御用マイコン 5 0 4 は認証完了信号を出力し、該認証完了信号は、信号処理回路 5 0 3、送受信回路 5 0 2、アンテナ 5 0 1 を介して認証装置から出力される。認証装置から出力された認証完了信号は、インターネットなどを通じて伝達される。なお、認証装置から出力された認証完了信号を、インターネットを介さず直接相手先に送信しても良い。

【0120】

本実施例の構成は、実施例1または2と組み合わせて実施することが可能である。

【0121】

(実施例4)

次に本発明で用いられる認証装置の1つである、携帯情報端末について述べる。図9に示すのは本実施例の携帯情報端末であり、2701は表示用パネル、2702は操作用パネルである。表示用パネル2701と操作用パネル2702は接続部2703において接続されている。そして接続部2703における、表示用パネル2701のセンサー内蔵ディスプレイ2704が設けられている面と操作用パネル2702の音声入力部2708が設けられている面との角度 θ は、任意に変えることができる。

【0122】

表示用パネル2701はセンサー内蔵ディスプレイ2704を有している。センサー内蔵ディスプレイ2704は画像の読み取りと、画像の表示との、2つの機能を併せ持っている。本実施例ではセンサー内蔵ディスプレイ2704にはELディスプレイが用いられている。

【0123】

また図9に示した携帯情報端末は電話としての機能を有しており、表示用パネル2701は音声出力部2705を有しており、音声は音声出力部2705から出力される。

【0124】

操作用パネル2702は操作キー2706、電源スイッチ2707、音声入力部2708を有している。なお図9では操作キー2706と電源スイッチ2707とを別個に設けたが、操作キー2706の中に電源スイッチ2707が含まれる構成にしても良い。音声入力部2708において、音声が入力される。

【0125】

なお図9では表示用パネル2701が音声出力部2705を有し、操作用パネル2702が音声入力部2708を有しているが、本実施例はこの構成に限定さ

れない。表示用パネル 2 7 0 1 が音声入力部 2 7 0 8 を有し、操作用パネルが音声出力部 2 7 0 5 を有していても良い。また音声出力部 2 7 0 5 と音声入力部 2 7 0 8 とが共に表示用パネル 2 7 0 1 に設けられていても良いし、音声出力部 2 7 0 5 と音声入力部 2 7 0 8 とが共に操作用パネル 2 7 0 2 に設けられていても良い。

【 0 1 2 6 】

なおセンサー内蔵ディスプレイ 2 7 0 4 は、携帯情報端末の周りの明るさ（照度）を測定し、自動的に輝度を調整する機能を有していても良い。また図 9 に示した本実施例の携帯情報端末は、センサー内蔵ディスプレイ 2 7 0 4 において周りの明るさ（照度）を測定することができるが、センサー内蔵ディスプレイ 2 7 0 4 とは別個に CCD 等のセンサ部を設けて、該センサ部において周りの照度を測定し、センサー内蔵ディスプレイ 2 7 0 4 の輝度を調整するようにしても良い。

【 0 1 2 7 】

また、携帯情報端末のセンサー内蔵ディスプレイ 2 7 0 4 は、電源投入時、操作キー 2 7 0 6 を操作している時、または電話の着信があった時に、自動的に輝度が高くなるようにし、通話している時、操作キー 2 7 0 6 を操作し終わってから一定の時間が過ぎた時に、自動的に輝度を下げるようにしても良い。これによって、携帯情報端末自体の消費電力を抑えることが可能になる。

【 0 1 2 8 】

またある一定の時間以上、操作キー 2 7 0 6 を操作しなかったり、電話が着信しなかったりすると、自動的にセンサー内蔵ディスプレイ 2 7 0 4 のみがオフの状態になって画像が表示されないようにすることも可能である。これによって、携帯情報端末自体の消費電力を抑えることが可能になる。

【 0 1 2 9 】

図 1 0、図 1 1 を用いて、図 9 で示した携帯情報端末の使用方法について説明する。図 1 0 に示すように、図 9 で示した携帯情報端末によって認証を行う場合には、手のひらをセンサー内蔵ディスプレイ 2 7 0 4 に覆いかぶせるようにして使用する。認証は操作キー 2 7 0 6 でキー操作を行うとともに、使用者の手相を

センサー内蔵ディスプレイ 2 7 0 4 が読み取り、認証作業を行う。

【 0 1 3 0 】

なお図 1 0 では操作キー 2 7 0 6 を人差し指で操作している例について示したが、図 1 1 に示すように、親指で操作キー 2 7 0 6 を操作することも可能である。なお操作キー 2 7 0 6 は操作用パネル 2 7 0 2 の側面に設けても良い。操作は片手（きき手）の人差し指のみ、または親指のみでも可能である。

【 0 1 3 1 】

以下に図 9 に示した携帯情報端末の構成と、その動作について説明する。

【 0 1 3 2 】

図 1 2 は本実施例の携帯情報端末のブロック図である。この携帯情報端末はアンテナ 9 0 1、送信受信回路 9 0 2、信号を圧縮伸張化、符号化する信号処理回路 9 0 3、制御用マイコン 9 0 4、フラッシュメモリ 9 0 5、操作キー 9 0 6、音声入力回路 9 0 7、音声出力回路 9 0 8、マイク 9 0 9、スピーカ 9 1 0などを有している。そしてさらに、センサー 9 1 1、照合回路部 9 1 2などを有している。

【 0 1 3 3 】

音声入力部 2 7 0 8 から入力された音声は、マイク 9 0 9 に入力され、アナログ信号として音声入力回路 9 0 7 に入力される。音声入力回路 9 0 7 に入力されたアナログ信号は増幅された後デジタル信号に変換され、信号処理部 9 0 3 に入力される。信号処理部 9 0 3 において圧縮伸張化、符号化されたデジタル信号は、送受信回路 9 0 2 において周波数を変えられて、場合によっては増幅されて、アンテナ 9 0 1 から送信される。

【 0 1 3 4 】

またアンテナ 9 0 1 において受信した音声情報を有するデジタル信号は、送受信回路 9 0 2 において周波数を変えられて、場合によっては増幅されて、信号処理部 9 0 3 に入力される。信号処理部 9 0 3 に入力されたデジタル信号は圧縮伸張化、符号化され、音声出力回路 9 0 8 に入力される。音声出力回路 9 0 8 に入力されたデジタル信号はアナログ信号に変換された後増幅され、スピーカ 9 1 0 から出力され、音声出力部 2 7 0 8 から音声として使用者の耳に入力される。

【 0 1 3 5 】

操作キー 9 0 6 を操作することによって、制御用マイコン 9 0 4 がセンサー 9 1 1 を制御し、使用者の生体情報を読み取らせる。なお本実施例では、生体情報として、掌紋または指紋を用いる例について説明する。センサー 9 1 1 で読み取った使用者の生体情報（照合用生体情報）は、照合回路部 9 1 2 に入力される。

【 0 1 3 6 】

照合回路部 9 1 2 に入力された照合用生体情報は、A/Dコンバータ 9 1 3 においてデジタル信号に変換される。デジタル信号に変換された照合用生体情報は、DSP（デジタルシグナルプロセッサ）9 1 4 に入力され、信号処理される。信号処理とは具体的には、生体情報をより判別しやすくするため、微分フィルタなどを用い映像の濃淡が変わるところを際立たせることである。得られた照合用生体情報は DSP 9 1 4 内部で数値化され、比較回路 9 1 5 に入力される。

【 0 1 3 7 】

比較回路 9 1 5 はフラッシュメモリ 9 0 5 に記憶されている基準用生体情報と、DSP 9 1 4 内部で数値化され比較回路 9 1 5 に入力された照合用生体情報とを比較し照合する。

【 0 1 3 8 】

生体情報を照合する方法としては、基準用生体情報と照合用生体情報のそれぞれの特徴を比較して照合する特徴照合方式と、該二つの生体情報を直接比較する画像マッチング方式があるが、どちらの方式を用いても良い。また基準用生体情報は 1 つだけではなく、手の向きを多少変えるなどして、複数備えたほうがより確実な認証が可能となる。

【 0 1 3 9 】

ここで合致が見られれば、制御用マイコン 9 0 4 は認証完了信号を出力し、該認証完了信号は、信号処理回路 9 0 3、送受信回路 9 0 2、アンテナ 9 0 1 を介して携帯情報端末から出力される。携帯情報端末から出力された認証完了信号は、インターネットなどを通じて伝達される。なお、携帯情報端末から出力された認証完了信号を、インターネットを介さず直接相手先に送信しても良い。

【 0 1 4 0 】

なお本発明で用いられる認証装置は、本実施例で示した構成の携帯情報端末に限定されない。また本実施例で示した携帯情報端末は、指紋または掌紋を生体情報として利用しているが、声紋を生体情報として利用する構成を有していても良い。

【 0 1 4 1 】

なお、本実施例は、実施例 1 ～ 3 を組み合わせて実施することが可能である。

【 0 1 4 2 】

(実施例 5)

本実施例は本発明を使用する状況を述べるものである。目的とする通信が取引などの営利のためになす経済行為に用いられる場合において、認証が生体情報までの高度な認証が不要な場合は本発明を使用しないこともありえる。小額の金銭移動などの場合は必ずしも必要ではない。

【 0 1 4 3 】

このため、認証の有無が選択できること、たとえば金銭が高額な移動が伴う場合のみに選択的に認証が出来るようにすることも可能である。相手先の状況に合わせて使用することや、あらかじめ認証装置の制御マイコン上に判定基準を設定しておき、数値が一定値を超えた場合のみ使用することが可能である。また、認証結果が必要な場合のみ、認証完了信号をインターネットで相手先（または管理者）伝達することも可能である。

【 0 1 4 4 】

なお、本実施例は、実施例 1 ～ 実施例 4 と組み合わせて実施することが可能である。

【 0 1 4 5 】

(実施例 6)

本発明に用いられる認証装置として、様々な電子機器を用いることができる。

【 0 1 4 6 】

図 1 3 (A) はパーソナルコンピューター（パソコン）であり、本体 2 5 0 1、筐体 2 5 0 2、表示部 2 5 0 3、キーボード 2 5 0 4、センサー 2 5 0 5 等を含む。本発明では、センサー 2 5 0 5 を用い、パーソナルコンピューター内に生

体情報を取り込むことができる。

【0147】

なお本実施例では、指紋または掌紋を生体情報として利用する例について示したが、音声入力部を設けて声紋を生体情報として利用する構成にしても良い。またセンサー2505と音声入力部を両方設けて、指紋または掌紋と、声紋とを共に利用する構成にしても良い。

【0148】

図13(B)は携帯電話であり、本体2601、音声出力部2602、音声入力部2603、表示部2604、操作キー2605、アンテナ2606を含んでいる。通常の電話をかける場合は表示部2604に相手先の電話番号や、電波の受信状態などが表示される。また、インターネットを使用する場合には、相手先の必要情報が表示されることになる。そして表示部2604はセンサーとしても機能し、表示部2604において生体情報を取り込むことが可能である。

【0149】

また、図13(B)に示した携帯電話は、表示部2604がセンサーとしての機能とディスプレイとしての機能を併せ持っていたが、表示部2604をディスプレイとしてのみ利用し、センサーを別個に設ける構成にしても良い。

【0150】

なお本発明で用いられる認証装置は本実施例で示した電子機器に限定されない。生体情報を取り込み、該生体情報をあらかじめ記憶されている生体情報と照合し、照合が合致したら相手先に認証が終了したことを知らせる機能を有していればよい。

【0151】

【発明の効果】

上述したように、本発明は生体情報を用いて認証作業を行うため、パスワードが本人以外の第三者に漏洩して、本人であることの確認が行われなくなる可能性がなくなる。よって、認証作業によって使用者が本人であることの確実性を高くすることができる。

【0152】

そして、認証作業の際に、使用者と相手先（または管理者）との間においてデータをやりとりする回数が抑えられるため、データの送受信に必要なコストを抑えることができ、何らかのエラーにより通信が途絶えて認証作業を再び最初から行うという繁雑さを回避することができる。

【0153】

さらに、使用者の生体情報を用いて認証作業を行うため、使用者がパスワードを忘れて相手先に問い合わせたり、パスワードを頻繁に書き換えたりする必要がなくなる。

【0154】

また一般的に生体情報は、パスワードに比べて情報量が大きい。しかし本発明では、本人または使用者の生体情報を、データとして相手先（または管理者）に直接送信する必要がないので、相手先（または管理者）とのデータの送受信に必要な時間の長さを抑えることができ、コストも抑えることができる。

【0155】

また本発明では、認証作業を行う全ての人の基準用生体情報を、相手先（または管理者）が保存しておく必要がないので、生体情報の情報量がパスワードに比べて大きくても、相手先（または管理者）の負担が重くなることがない。そして、個人で基準用生体情報を保存しているので、セキュリティが破られたときに漏洩する基準用生体情報の数（この場合、同一の人が有する全ての生体情報を一と数える）を、認証作業を行う全ての人の基準用生体情報を相手先（または管理者）に保存しておく場合に比べて、抑えることが可能である。

【図面の簡単な説明】

【図1】 本発明の通信システムのフロー。

【図2】 読み取る掌紋または指紋の位置を示す図。

【図3】 生体情報の照合の関係図。

【図4】 生体情報の照合の関係図。

【図5】 認証が完了した後のフロー。

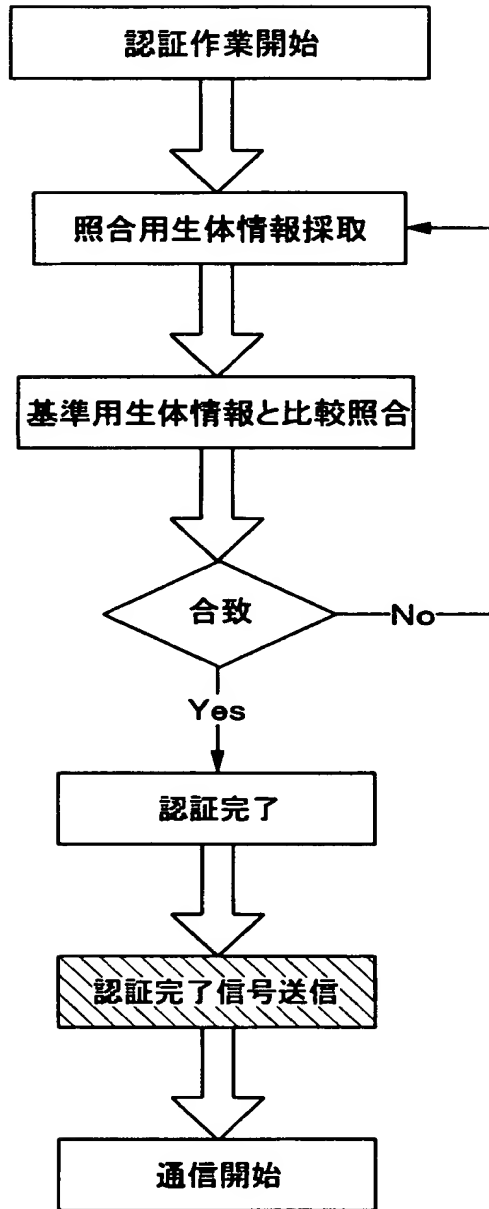
【図6】 基準用生体情報を書き換える際の手書き換え作業のフロー。

【図7】 認証装置の構造を示すブロック図。

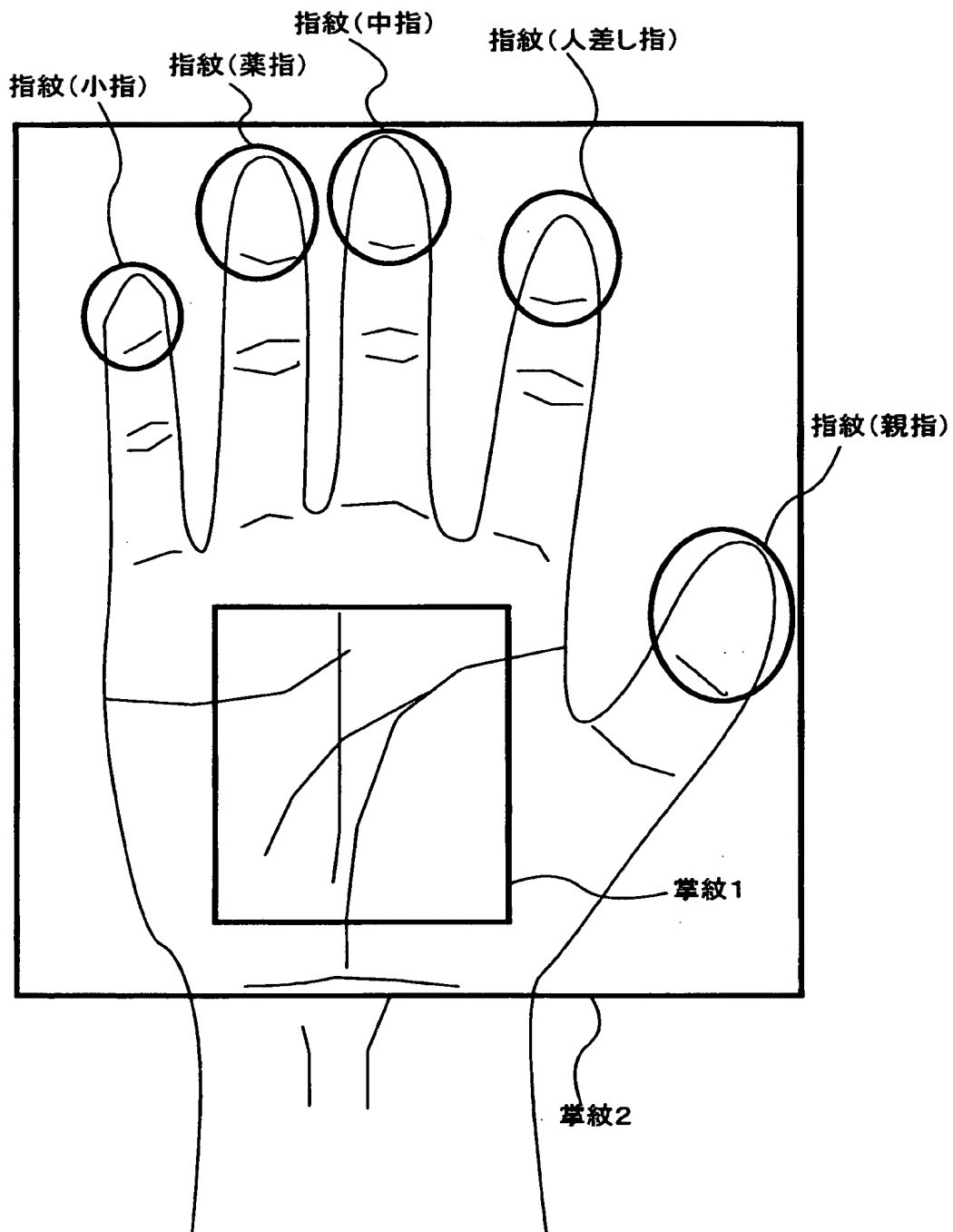
- 【図 8】 認証装置の構造を示すブロック図。
- 【図 9】 認証装置の一例である携帯情報端末の外観図。
- 【図 1 0】 認証装置の一例である携帯情報端末の使用例。
- 【図 1 1】 認証装置の一例である携帯情報端末の使用例。
- 【図 1 2】 認証装置の一例である携帯情報端末の構造を示すブロック図。
- 【図 1 3】 認証装置の一例である電子機器の図。
- 【図 1 4】 従来の認証のフロー。

【書類名】 図面

【図 1】



【図 2】

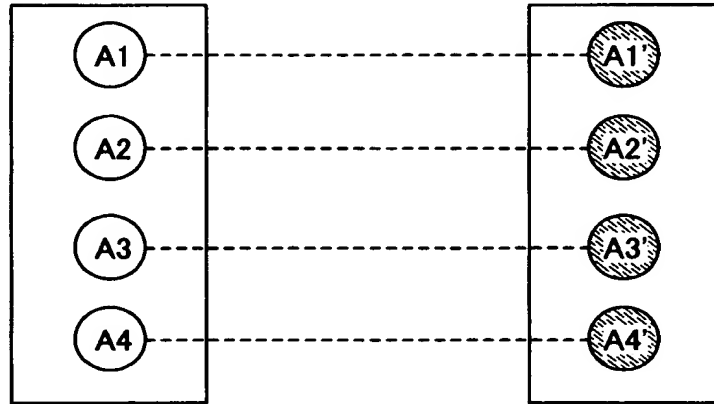


【図 3】

(A)

基準用生体情報

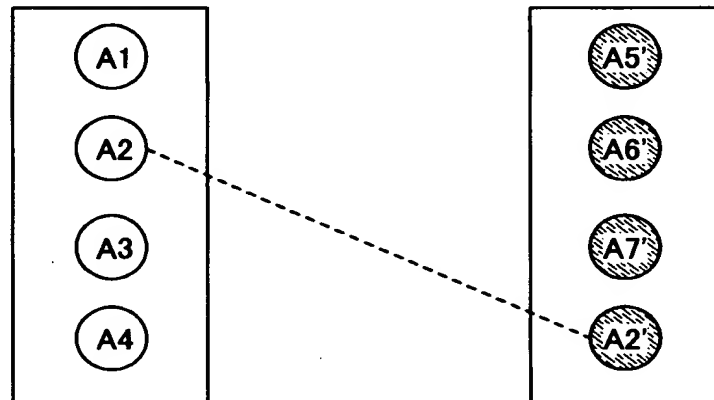
照会用生体情報



(B)

基準用生体情報

照会用生体情報

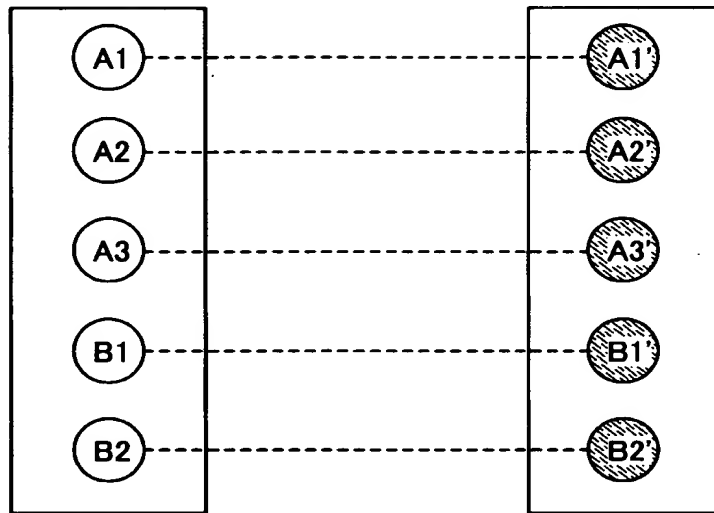


【図 4】

(A)

基準用生体情報

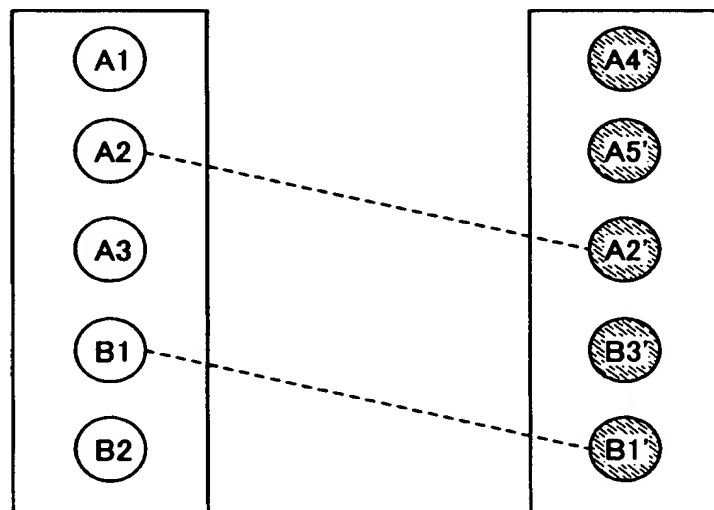
照会用生体情報



(B)

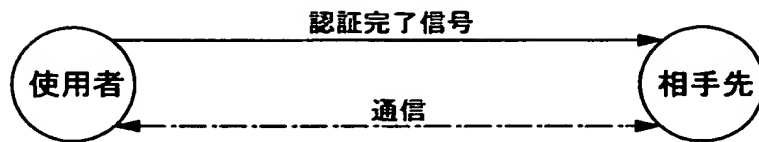
基準用生体情報

照会用生体情報

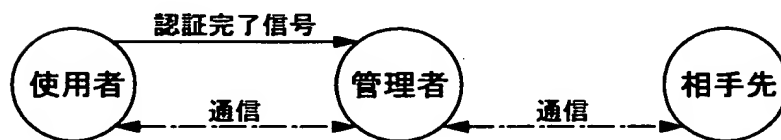


【図 5】

(A)



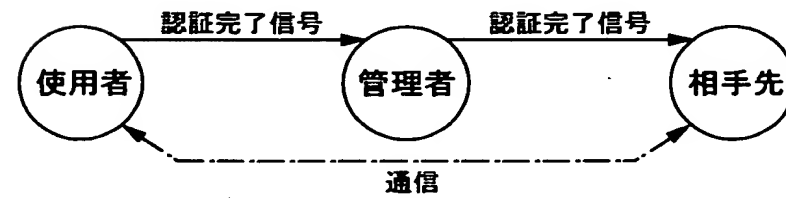
(B)



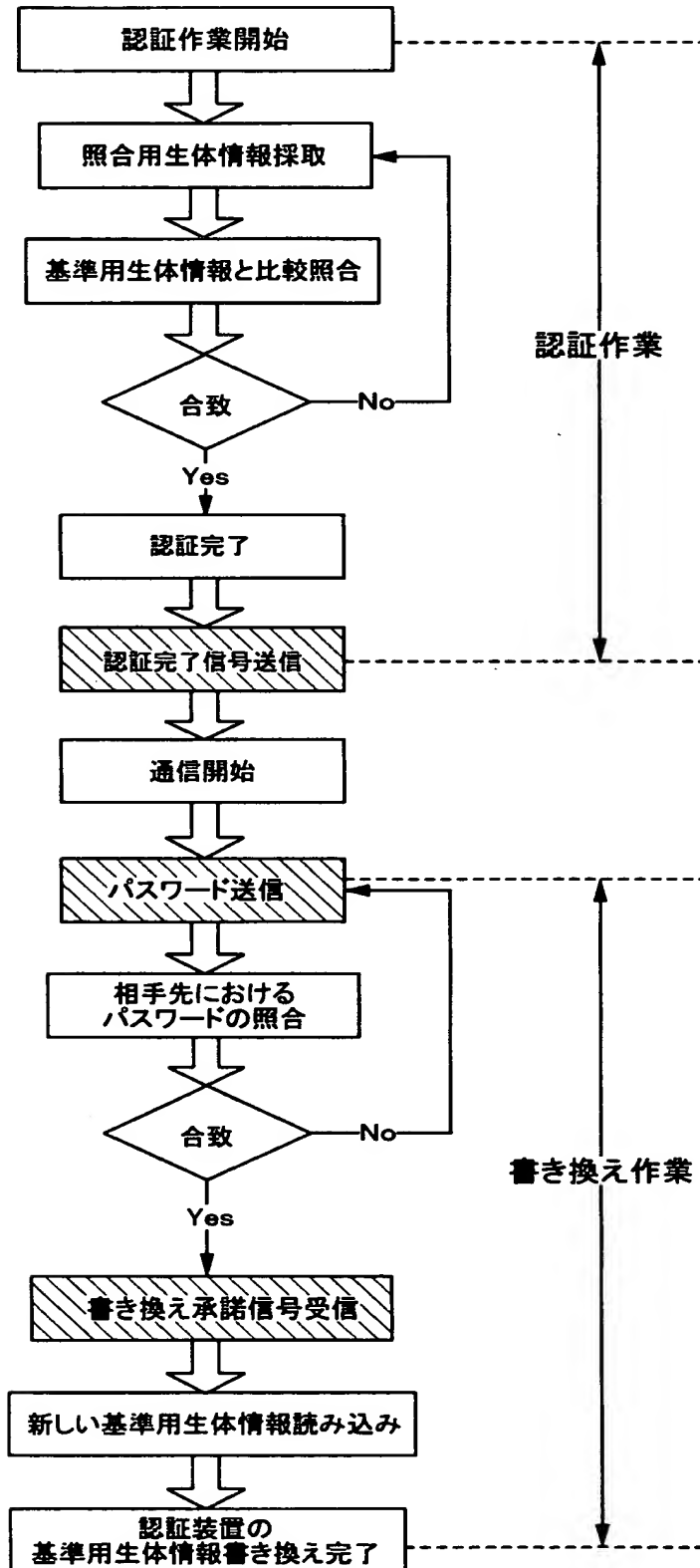
(C)



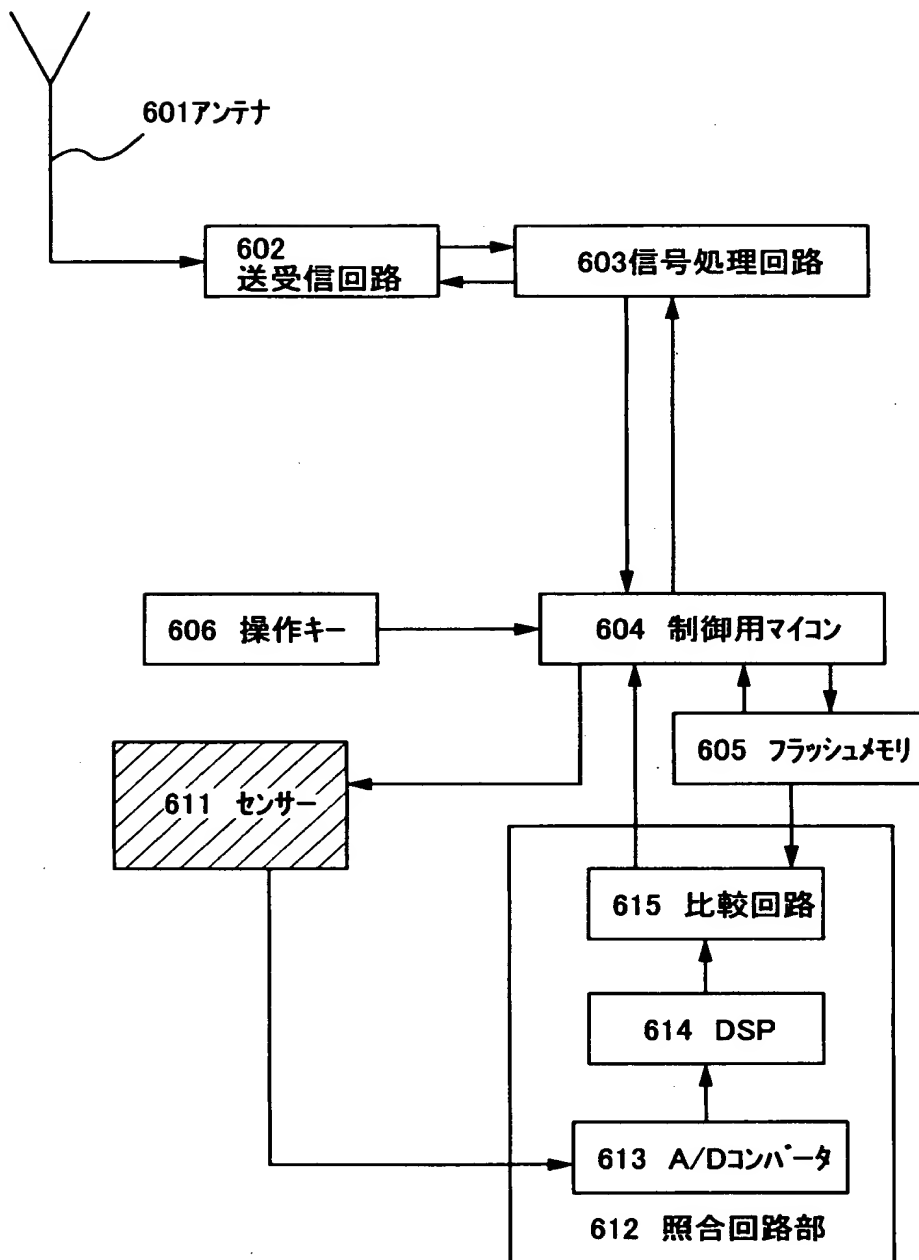
(D)



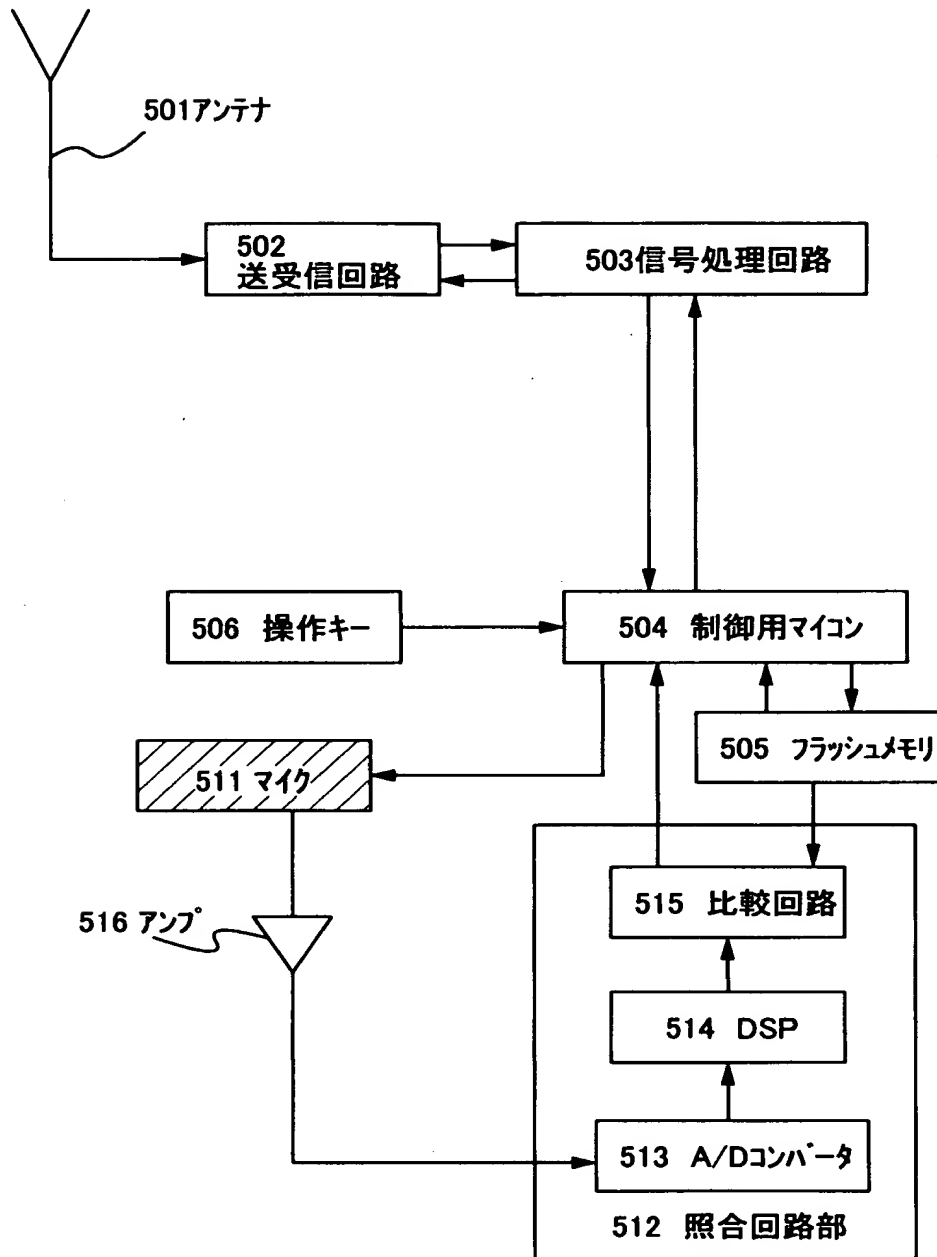
【図 6】



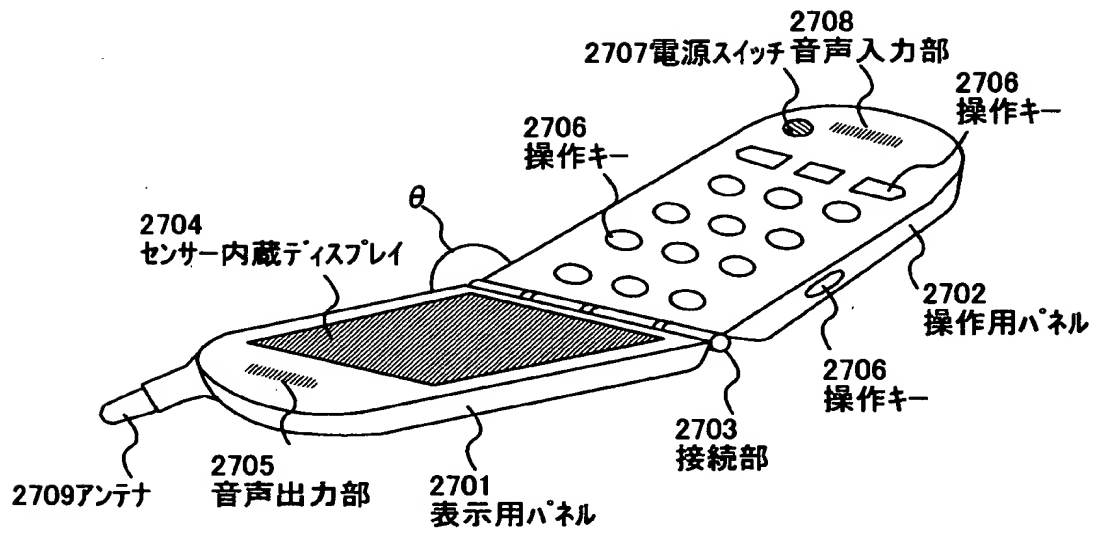
【図 7】



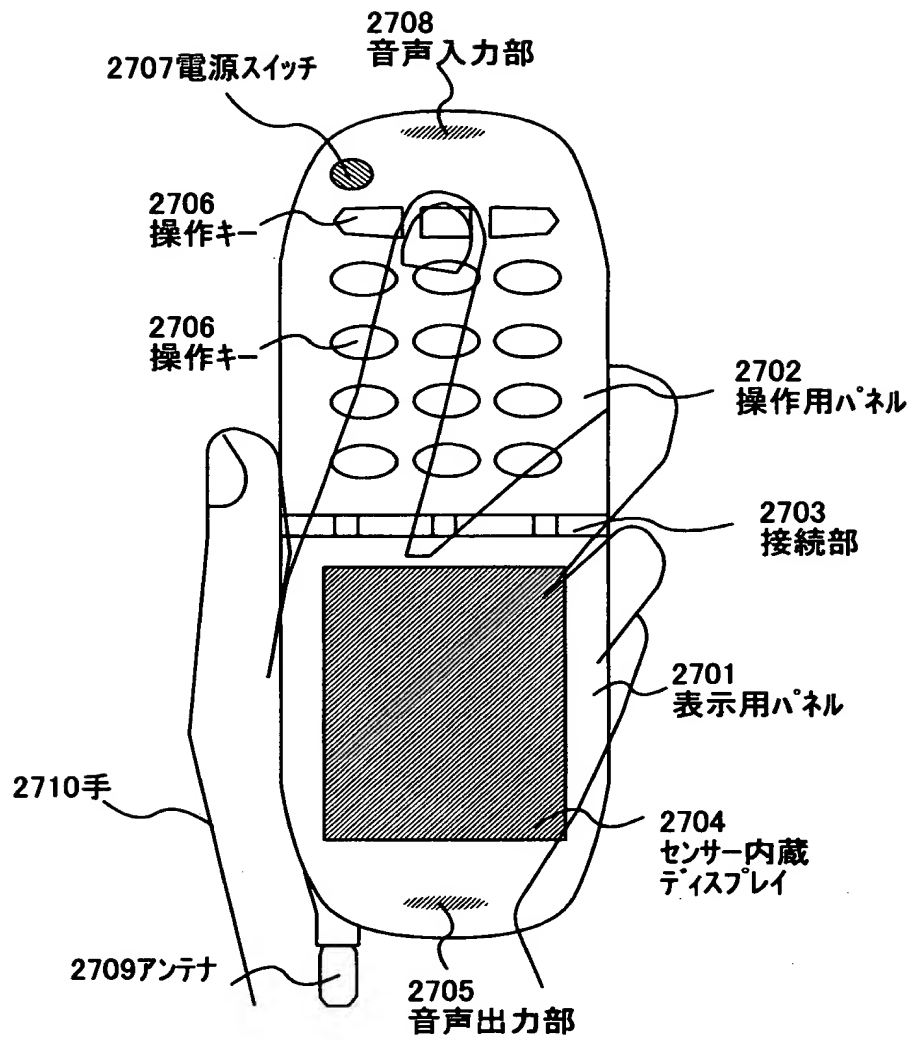
【図 8】



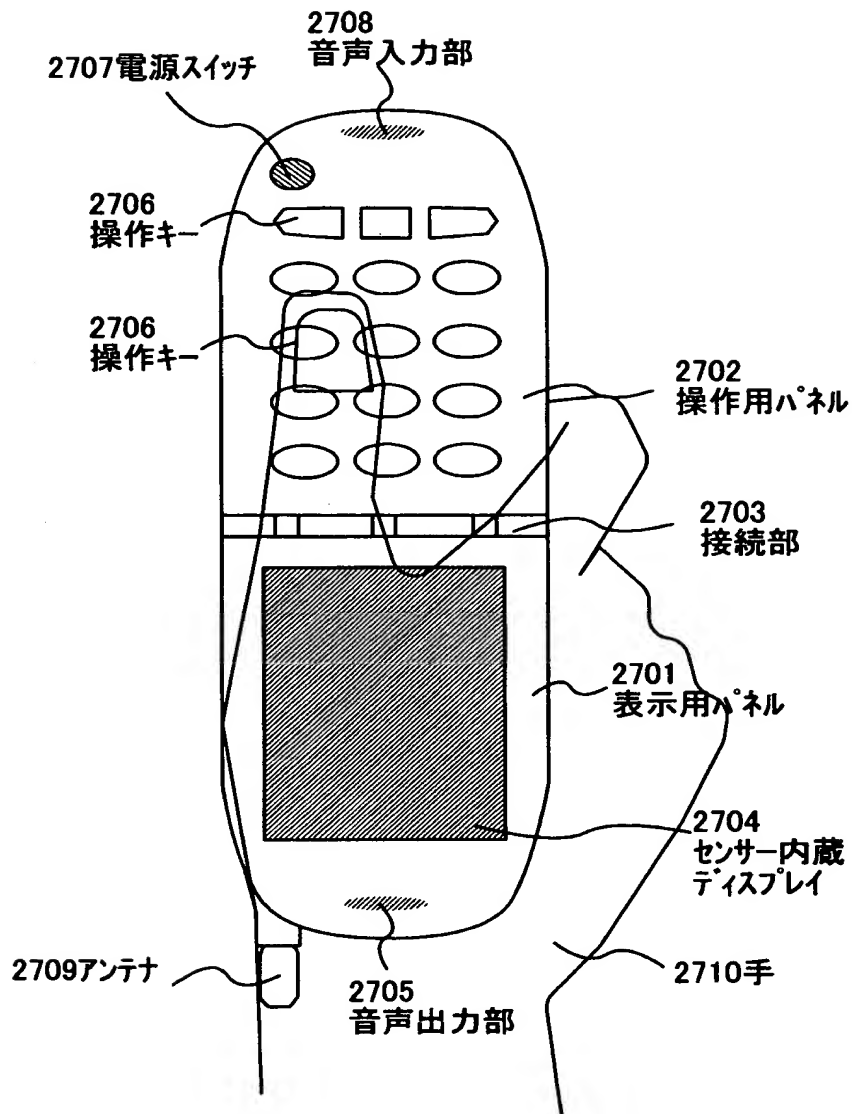
【図 9】



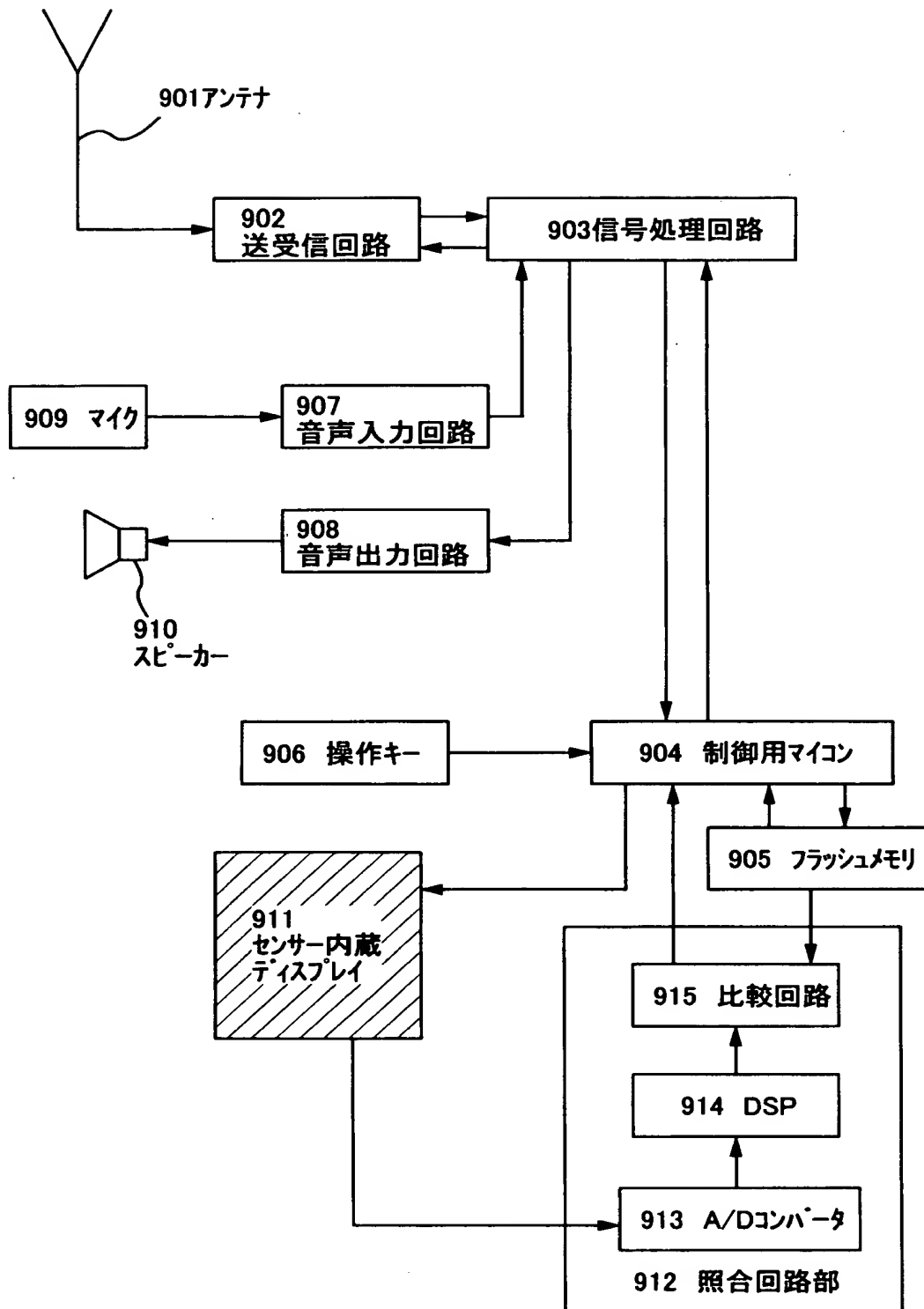
【図 1 0】



【図 1 1】

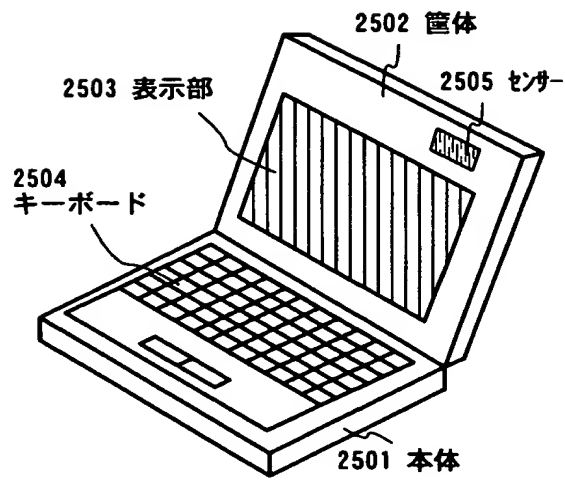


【図 1 2】

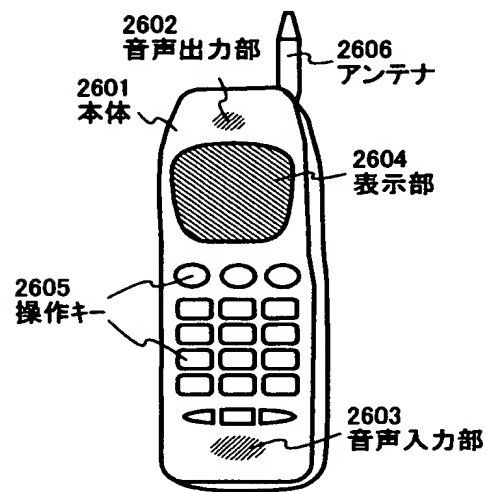


【図 1 3】

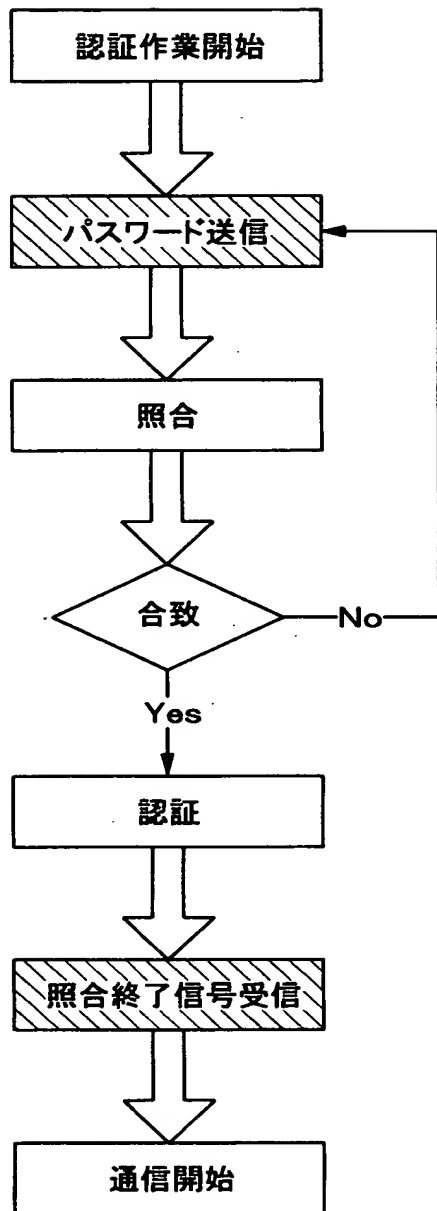
(A)



(B)



【図 1 4】



【書類名】 要約書

【要約】

【課題】 使用者の識別が容易な認証システムを提供する。

【解決手段】 基準用生体情報を記憶する手段と、前記使用者の照会用生体情報を読み取る手段と、前記照会用生体情報を前記基準用生体情報と照合する手段と、前記照合が合致した場合相手先に合致したことをデータとして送る手段と、を有することを特長とする認証システム。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000153878]

1. 変更年月日	1990年 8月17日
[変更理由]	新規登録
住 所	神奈川県厚木市長谷398番地
氏 名	株式会社半導体エネルギー研究所